The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	NO. CR19-159-RSL GOVERNMENT'S CONSOLIDATED MOTIONS *IN LIMINE*

The United States of America, by and through Nicholas W. Brown, United States Attorney for the Western District of Washington, and Andrew C. Friedman, Jessica M. Manca, and Tania M. Culbertson, Assistant United States Attorneys for said District, hereby submits its pretrial motions *in limine* in the above-captioned case, under local criminal rule 23.2.[1]

The government seeks to exclude certain evidence and argument by the defense at trial. First, the government moves to exclude evidence or argument regarding potential or actual cyber-security vulnerabilities of victim companies, including Capital One, other than the vulnerability exploited by Thompson in this case.

[1] Undersigned counsel and counsel for the defendant, Paige Thompson, met and conferred about these motions by phone on May 18 and 20, 2022.

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Second, and relatedly, the government moves to exclude evidence or argument regarding a note given to an Amazon employee by an unknown person in mid-to-late May 2019, describing a potential Amazon Web Services (AWS) security vulnerability unrelated to the security vulnerability exploited by the defendant in this case.

Third, the government moves to exclude evidence relating to an $80 million civil penalty imposed against victim Capital One by the Office of the Comptroller of the Currency in August 2020.

Fourth, the government also moves to exclude evidence regarding a pending $190 million settlement by Capital One of a class-action lawsuit brought on behalf of Capital One's customers whose personal identifying information (PII) was stolen by Thompson.

Fifth, the government moves to exclude evidence and argument from Thompson's mental health expert except as it bears directly on her capacity to form the specific intent for the crimes for which she is being tried.

The government requests the opportunity to supplement these motions should any additional legal issues arise requiring the Court's intervention. Because the defendant has not yet produced any reciprocal discovery under Fed. R. Crim. P. 16(b), the government also requests the opportunity to supplement these motions to address issues triggered by such discovery.

DISCUSSION

A. Motion *in Limine* No. 1: The Court should exclude evidence and argument regarding cyber-security vulnerabilities at Capital One or other victim companies that are different from the vulnerability Thompson exploited in this case

The government anticipates that the defense will seek to question witnesses or admit evidence regarding cyber-security vulnerabilities at Capital One or other victim companies that are unrelated to the specific vulnerability Thompson used here. The Court should exclude any such evidence or argument as irrelevant and because it will confuse the issues, mislead the jury, waste time, and because it risks unfair prejudice. *See* Fed. R. Evid. 401–403.

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The government does not know what potential evidence of unrelated cyber-security vulnerabilities the defense might seek to introduce, or on what basis. To be sure, any company that operates in any significant capacity online (such as the victim companies in this case) must engage in a continual process of identifying and mitigating potential vulnerabilities. But the fact that victim companies may have had other vulnerabilities at the time that Thompson identified and exploited the specific vulnerability at issue here, or may have had other vulnerabilities in the past, is not relevant to any fact of consequence to the determination of this case because the existence of other vulnerabilities does not "bear on any issue involving the elements of the charged offense[s]." *United States v. Dean*, 980 F.2d 1286, 1288 (9th Cir. 1992); *see also id.* ("For evidence to be relevant it must 'be probative of the proposition it is offered to prove, and . . . the proposition to be proved must be one that is of consequence to the determination of the action.'" (quoting *United States v. Click*, 807 F.2d 847, 850 (9th Cir. 1987)).

The defense may argue that evidence of other cyber-security vulnerabilities is relevant because it shows that the victim companies in this case were negligent or lax in their cyber-security practices and left themselves open to attacks such as Thompson's. The Court should reject this argument because in the criminal context, of course, victim negligence is irrelevant.[2] The Ninth Circuit has repeatedly so held, including specifically in fraud cases. *See, e.g.*, *United States v. Lindsey*, 850 F.3d 1009, 1015 (9th Cir. 2017) ("We join several of our sister circuits in holding that a victim's negligence is not a defense to wire fraud."); *United States v. Ellison*, 704 F. App'x 616, 620 (9th Cir. 2017) ("a victim's negligence is not a defense" to securities fraud); *United States v.*

[2] Such an argument would also likely violate Rule 404's prohibition against admitting "other acts" evidence to "prove a person's character in order to show that on a particular occasion the person acted in accordance with the character," since the argument asks the jury to infer that a particular company was negligent in its cybersecurity generally, and therefore must have been negligent on a particular occasion as well. *See* Fed. R. Evid. 404(b)(1). Security vulnerabilities not relating to Thompson's intrusion are, by definition, not inextricably intertwined with her intrusion, and therefore could only be offered as "other acts" evidence. Further, the defense has not provided notice of intent to admit evidence under Rule 404(b).

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Palamarchuk, 791 F. App'x 658, 660 (9th Cir. 2019) ("neither individual victim lender negligence nor an individual victim lender's intentional disregard of relevant information is a defense to mail fraud").

Other circuits have reached similar conclusions in fraud cases. *See, e.g.*, *United States v. Powell*, 509 F. App'x 958, 967 (11th Cir. 2013) ("Likewise, whether the lenders negligently created an environment of lax lending standards is irrelevant. Contributory negligence is not a defense to the crime of fraud."); *United States v. Coyle*, 63 F.3d 1239, 1244 (3d Cir. 1995) ("[T]he negligence of the victim in failing to discover a fraudulent scheme is not a defense to criminal conduct."); *United States v. Moore*, 923 F.2d 910, 917 (1st Cir. 1991) ("[I]t is not a defense that the bank might have prevented its losses had it better internal controls or procedures."); *United States v. Winkle*, 477 F.3d 407, 418 (6th Cir. 2007) (approving the exclusion of an FDIC report that criticized the bank fraud victim's failure to detect a fraud scheme); *United States v. Rennert*, 374 F.3d 206, 213 (3d Cir. 2004) ("fraud victim's negligence or lack of diligence in uncovering the fraud is not a defense"); *United States v. Thomas*, 377 F.3d 232, 243-44 (2d Cir. 2004) (affirming restrictions on cross of victim; rejecting defendant's argument that victim's foolishness vitiated defendant's fraudulent intent); *United States v. Frenkel*, 682 F. App'x 20, 22 (2d Cir. 2017) ("A victim's negligence is not a defense under the federal fraud statutes." (citations omitted)).

The same principle that a victim's negligence is not a defense also applies to the charges of Computer Fraud and Abuse set forth in Counts 2 and 4-8. Each of those counts requires proof that Thompson acted "without authorization." "A person uses a computer 'without authorization' when the person has not received permission from the owner, person [], or entity which controls the right of access to the computer for any purpose." Ninth Circuit Model Jury Instruction 15.21. As this Court already has held in this case, "Ninth Circuit precedent . . . makes clear that 'authorization' is something that only the owner of the computer or similar authority can provide." Dkt. No. 226 (Order

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Denying Motion to Dismiss Counts 2 through 8) at 5 (noting also, that Thompson had not cited any case where a user's authorization was granted by mistake).

In addition to being irrelevant, this type of evidence is also inadmissible under Federal Rule of Evidence 403 because any probative value would be substantially outweighed by the danger of unfair prejudice, confusion of the issues, and misleading the jury. Allowing broad inquiry into the cyber-security practices of victim companies relating to vulnerabilities not at issue in this case—rather than the conduct of the defendant—would be unfairly prejudicial because it would encourage the jury to render a verdict based on considerations other than Thompson's guilt or innocence. Such evidence would serve only to create the impression that the victim companies were negligent and deserved to be hacked.[3]

Furthermore, this case undoubtedly will require the jury to consider a large amount of technical evidence simply to understand the vulnerability Thompson actually exploited and the steps she took in order to do so. Allowing evidence and argument regarding irrelevant vulnerabilities that Thompson is not charged with exploiting not only will confuse and mislead the jury with respect to the complicated facts it will be tasked with finding; it will also waste a great deal of trial time. Hindsight challenges to any of the victim companies' actions with respect to other vulnerabilities, and challenges to their internal cyber-security practices more generally, should be excluded.

B. Motion *in Limine* No. 2: The Court should exclude evidence or argument regarding a note given to an Amazon employee by an unknown person in May 2019.

The government anticipates that the defense will seek to question witnesses or admit evidence regarding a handwritten note of unknown origin given to an Amazon

[3] This danger is particularly acute for Capital One, given the animus that some people may feel towards large financial institutions generally and credit card companies specifically.

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

employee at an internal Amazon conference in May 2019, and then shared by Amazon with Capital One.[4] The note, written and delivered by an unknown person, reads:

> Open Socks Proxy
> 35.162.65.136
> Can Hit IMS - lots of
> Security Credentials

All proxies are not the same. The vulnerability that Thompson exploited was specific to web-based traffic on a reverse proxy. A SOCKS proxy is different from a reverse proxy in that it operates at different communication layer and on a different communication protocol. The security vulnerability that Thompson exploited in this case did not involve a SOCKS proxy. *See* Dkt. No. 267 (Government's Redacted Trial Brief explaining the vulnerability Thompson exploited). A SOCKS proxy is not web-based; it is more akin to a virtual private network (VPN) tunnel. A SOCKS proxy operates at a session level (between two machines); whereas the exploit that Thompson used was on the application level (between the user and the software application). Unsurprisingly, when Capital One received this note, it looked for open SOCKS proxies. It did not find an open SOCKS proxy (or similar vulnerability) and subsequently dismissed the note as a false alarm. In short, the note does not describe the security vulnerability Thompson used against Capital One.

Furthermore, Amazon received the note approximately two months after Thompson exfiltrated Capital One's data. The damage had already been done, which further reduces the probative value of this evidence. Finally, the government is not aware of any evidence indicating that Thompson was involved with the writing or dissemination of this note to Amazon, and the defense has not produced any such evidence in discovery.

Accordingly, the note is not relevant to any of the issues in this case—it addresses (in vague terms) a potential AWS security vulnerability not used by Thompson to hack any of the victims from whom she stole data and computing power, it was given to an

[4] Amazon shared the note with Capital One because it recognized the IP address in the note as one of numerous AWS IP addresses used by Capital One.

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Amazon employee several months after Thompson downloaded the stolen victim data, and there is no evidence connecting Thompson to the note. For all these reasons, the note and surrounding investigation have no bearing on any fact of consequence to the determination of this case. *See* Fed. R. Evid. 401, 402.

The government does not know on what basis the defense would try to introduce evidence or make arguments concerning this note, but any such evidence or argument—even if the defense could show even minimal probative value—would nevertheless be a waste of time and would tend to confuse and mislead the jury. As such it should also be excluded under Federal Rule of Evidence 403.

As the Court is aware, this case involves a great deal of complex technical information but ultimately it turns on the evidence found on Thompson's computer (including computer scripts showing the security vulnerability she exploited, the attack vector she used, and a copy of the data she stole) and Thompson's own admissions of what she did. It does not turn on other potential AWS security vulnerabilities that an unknown person claimed may have existed around the time Thompson hacked AWS customers. And that is true even if the note purporting to identify a security vulnerability cited an IP address used by one of the victims in this case. *See, e.g.*, *United States v. Spencer*, 1 F.3d 742, 745 & n.2 (9th Cir. 1992) (no abuse of discretion to exclude evidence of subsequent arrest report for the owner of the car in which the defendant was a passenger because the district court properly "concluded that the risk of confusing the issues and wasting time outweighed the likely value of any inferences that could conceivably be drawn from the subsequent discovery of a different gun under a different seat in a different car (albeit a car owned by the same person who owned the car in which [the defendant] was a passenger)").

Here, given the complexity of the technical evidence that will be presented, there is a substantial danger that the jury will be confused by evidence of a note referencing an AWS IP address used by Capital One, but in relation to a different potential security vulnerability than the one Thompson exploited and where no evidence whatsoever links

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Thompson to the note. It would require a considerable amount of trial time to educate the jury on the differences between the network protocol Thompson used to hack the victims in this case and the SOCKS proxy network protocol referenced in the note, and then to explain the efforts Capital One took to investigate that vulnerability—time that ultimately would be wasted because the SOCKS proxy network protocol has no bearing on the facts of this case. Thus, absent a proffer of evidence from the defense linking Thompson to the note, the Court should exclude any evidence or argument concerning the note because it is not relevant and because of the danger it will confuse the issues, mislead the jury, and waste time.

Finally, the Court also should reject any argument by the defense that the note is relevant because it demonstrates negligence by AWS or Capital One. As discussed more fully above, in the criminal context victim negligence is irrelevant. *See Lindsey*, 850 F.3d at 1015.

C. Motion *in Limine* No. 3: The Court should exclude evidence of an $80 million penalty imposed by the Office of the Comptroller of the Currency on Capital One.

Based on Thompson's arguments to date, the government anticipates that Thompson will argue that she did not commit a crime, and will instead claim that Capital One is to blame for failing to secure its data. The government anticipates that Thompson will seek to point to the fact that the Office of the Comptroller of the Currency (the OCC) imposed an $80 million fine on Capital One following Thompson's breach to support her argument. The Court should exclude all evidence relating to the imposition of that penalty under Federal Rules of Evidence 401 and 403, and should exclude the OCC order itself as hearsay.

In this case, following Thompson's hack of Capital One, and Capital One's public disclosure of the breach in July 2019, the OCC conducted an investigation. In August 2020, the OCC and Capital One entered into a Consent Order, a copy of which is attached as Exhibit 1. That Consent Order contained findings by the OCC, which Capital One neither admitted nor denied, that:

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

> (1) In or around 2015, the Bank failed to establish effective risk assessment processes prior to migrating its information technology operations to the cloud operating environment. The Bank also failed to establish appropriate risk management for the cloud operating environment, including appropriate design and implementation of certain network security controls, adequate data loss prevention controls, and effective dispositioning of alerts.
>
> (2) The Bank's internal audit failed to identify numerous control weaknesses and gaps in the cloud operating environment. Internal audit also did not effectively report on and highlight identified weaknesses and gaps to the Audit Committee.
>
> (3) For certain concerns raised by internal audit, the Board failed to take effective actions to hold management accountable, particularly in addressing concerns regarding certain internal control gaps and weaknesses.
>
> (4) By reason of the foregoing conduct, the Bank was in noncompliance with 12 C.F.R. Part 30, Appendix B, "Interagency Guidelines Establishing Information Security Standards," and engaged in unsafe or unsound practices that were part of a pattern of 3 misconduct.
>
> (5) The Bank has begun addressing the identified corrective action and has committed to providing resources to remedy the deficiencies.

See Exhibit 1, at 2-3. Based upon those findings, the OCC assessed Capital One a civil penalty of $80 million. *See id*

The findings that Capital One engaged in unsafe and/or unsound practices are akin to findings that the bank was negligent. But, as noted in Motion *in Limine* No. 1, *supra* at pp. 3-5, even if Capital One was negligent, that is not a defense either to wire fraud or to the charge that Thompson accessed Capital One's computers without authorization. As a result, the evidence is not probative of any proposition of consequence, and it should be

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

excluded under Federal Rule of Evidence 401. *See also Dean*, 980 F.2d at 1288 (evidence that does not "bear on any issue involving the elements of the charged offense[s]" should be excluded).

Even if the Court were to disagree and consider the evidence relevant, it nevertheless should be excluded for two other reasons. First, the Consent Order itself is hearsay. "A court judgment is hearsay 'to the extent that it is offered to prove the truth of the matters asserted in the judgment.'" *United States v. Sine*, 493 F.3d 1021, 1024 (9th Cir. 2007) (quoting *United States v. Boulware*, 384 F.3d 794, 806 (9th Cir. 2004). The same is true of "findings of fact" underlying a judgment. Such findings are inadmissible hearsay unless a specific hearsay exception applies. *Id.*

Second, the probative value of the evidence would be substantially outweighed by the danger of unfair prejudice, confusion of the issues, and misleading the jury. *See* Fed. R. Evid. 403. An $80 million penalty is a large penalty. The fact that it was assessed by a government agency further increases the impact such testimony would have. If the jury were to hear evidence that Capital One had been assessed an $80 million penalty by the OCC, it might well incorrectly conclude that the fact, and magnitude, of the penalty suggested that the breach was Capital One's fault, rather than Thompson's. And it might not follow instructions and convict Thompson, even though the evidence will establish each and every element of the crimes with which Thompson is charged.

For all of these reasons, the Court should hold that the OCC's Consent Order, as well as the fact that the OCC imposed an $80 million regulatory penalty on Capital One, are inadmissible.

D. Motion *in Limine* No. 4: The Court should exclude evidence of the $190 settlement of a class action brought against Capital One

The government anticipates that, as part of her argument that Capital One is to blame for failing to secure its data, Thompson will also seek to introduce evidence that Capital One is in the process of settling a class action brought against it following

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Thompson's breach, for $190 million. The Court should exclude all evidence relating to this settlement under Federal Rules of Evidence 401, 403, and 408.

Following Thompson's breach of Capital One, a class action was filed against Capital One and Amazon alleging negligence, negligence *per se*, unjust enrichment, breach of express and implied contract, and declaratory judgment, as well as state statutory claims under state data breach notification and consumer protection statutes. *See In re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA) (E.D. Va.) (Docket No 332). In December 2021, the parties announced a settlement of that action. Under the terms of that settlement, a copy of which is attached as Exhibit 2, and which still is awaiting court approval, Capital One agreed to pay $190 million into a settlement fund to pay various class benefits, as well as costs, fees, and expenses. *See* Exhibit 2 at 11. Capital One did not admit any wrongdoing. *See id.* at 23-26.

The Court should exclude evidence of this settlement for multiple reasons. First, the negligence (and other violations) alleged in the class action are irrelevant to the issues in Thompson's criminal prosecution. *See* Motion *in Limine* No. 1, *supra* at pp. 3-5 (a victim's negligence is not relevant in a fraud or Computer Fraud and Abuse Act prosecution). As a result, the settlement is not probative of any proposition of consequence, and evidence regarding it should be excluded as irrelevant under Federal Rule of Evidence 401.

Second, any probative value of the evidence would be substantially outweighed by the danger of unfair prejudice, confusion of the issues, and misleading the jury. *See* Fed. R. Evid. 403. This is true for three reasons: Capital One did not admit any wrongdoing. As a result, the settlement stands on its own—it would be impossible for the jury accurately to discern the facts that led to it. In addition, the settlement is for a very large sum. A jury that heard that Capital One had paid a $190 million settlement would be likely to be misled and confused, and to conclude that Capital One was at fault and that Thompson was not at fault, despite evidence proving the requisite elements of all of the

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

charges against her. Finally, the legal claims addressed in the civil action (negligence, breach of contract, unjust enrichment, and consumer protection) are completely different from the elements of the crimes charged in the Indictment. It is misleading, prejudicial, and confusing to suggest that the issues that lead to liability the civil arena translate directly to a legal or factual defense in a criminal case.

Third, it is well established that evidence of settlements is inadmissible. Federal Rule of Evidence 408 provides that evidence of "furnishing, promising, or offering – or accepting, promising to accept, or offering to accept – a valuable consideration in compromising or attempting to compromise [a] claim" is "not admissible—on behalf of any party—either to prove or disprove the validity . . . of a disputed claim." Fed. R. Evid. 408. Here, the evidence would be offered by Thompson to suggest that Capital One was liable for the breach. That purpose directly violates Rule 408.

For all three of these reasons, the Court should exclude any evidence of the $190 settlement of the class action against Capital One.

E. Motion *in Limine* No. 5: Evidence regarding Thompson's mental health issues should be excluded unless such evidence relates directly to Thompson's mens rea for the charged offenses

As the Court is aware, the defense provided notice of its intent to introduce expert evidence relating to a mental condition that bears on the issue of guilt. *See* Fed. R. Crim. P. 12.2(a). That notice has an attendant discovery obligation: the defense must produce a written summary describing the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications. *See* Fed. R. Crim. P. 16(b)(1)(C). Initially, the defense's Rule 12.2 disclosure did not include an expert witness disclosure as required by rule. At the government's request, the defense supplemented its Rule 12.2 disclosure with a report that Dr. Matthew Goldenberg wrote in support of Thompson's motion for pretrial release in the fall of 2019.

Dr. Goldenberg's opinion is not the type of opinion that would typically be offered to support a mental health defense like diminished capacity. Dr. Goldenberg's evaluation and opinion were focused on a different issue than the one before the jury, specifically,

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

he opined about how Thompson's mental health was affected by her pretrial incarceration. Although Dr. Goldenberg offered an opinion relating to Thompson's mental condition, he did not opine on Thompson's mental state at the time she committed the acts for which she is being prosecuted. Nor did he explain how or why his opinion bears on the issue of guilt, or, more specifically how or why his mental health diagnoses would bear on Thompsons's intent to defraud.

Because of these omissions, the Court should exclude as irrelevant the bulk of Dr. Goldenberg's opinion as summarized in his report. At a minimum, Dr. Goldenberg's testimony be limited to his diagnostic impressions, and that the following sections of his report be excluded: (1) Current Medications; (2) Social History; (3) Academic History; (4) Substance Use History; (5) Suicidal Risk; (6) Details Regarding Her Gender Identity and Gender Transition; (7) Safety Issues Facing Transgender Individuals in Prison; and (8) Care Recommendations. Attached Exhibit 3 is a version of Dr. Goldenberg's report that highlights the portions of the report that the government believes should be excluded as irrelevant and prejudicial under Fed. R. Evid. 401, 402, and 403. Other witnesses should similarly be excluded from offering evidence of, or speculating about, Thompson's mental health history.

More broadly, while Dr. Goldenberg offers his diagnostic impression that Thompson struggles with certain mental health conditions, it is well established that expert testimony on a mental health condition is only admissible if it is offered to negate the mens rea element of a crime. *United States v. Pohlot*, 827 F.2d 889, 905-06 (3d Cir. 1987). As the proponent of the evidence, the defendant bears the burden of showing that the proffered testimony is offered to negate mens rea and not in support of an improper or irrelevant defense theory. *United States v. Brown*, 326 F.3d 1143, 1147 (10th Cir. 2003) ("The admission of such [psychological or psychiatric] evidence will depend on whether the defendant clearly demonstrates how such evidence would negate intent rather than

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

'merely present a dangerously confusing theory of defense more akin to justification and excuse.'") (quoting *United States v. Cameron*, 907 F.2d 1051, 1067 (11th Cir. 1990)).

There are a number of mental health conditions that may affect a person's judgment but do not negate intent to commit a crime. Indeed, "[o]nly in the rare case" will a defendant be so incapacitated by a mental condition that his or her mens rea is negated: "Mental illness rarely, if ever, renders a person incapable of understanding what he or she is doing." *Pohlot*, 827 F.2d at 900. For example, in *United States v. Andrews*, a wire fraud prosecution, the district court excluded evidence of a defendant's bipolar disorder because there was no evidence that this condition negated the mens rea of wire fraud (intent to defraud). 811 F. Supp. 2d 1158 (E.D. Pa. 2011). The Court collected and discussed a long series of cases in which expert testimony on bipolar disorder was excluded as irrelevant and unhelpful to the jury. *Id.* at 1172-74; *accord United States v. Worrell*, 313 F.3d 867, 870-75 (4th Cir. 2002); *United States v. Agnello*, 158 F. Supp. 2d 285, 289 (E.D.N.Y. 2011). Similarly, in *United States v. Brown*, the district court properly excluded expert testimony about a defendant's post-traumatic stress disorder because the proffered expert did not opine on how that condition was either related to or negated a specific intent element. 326 F.3d at 1147-48. Here, the defense has not even attempted—let alone carried its burden—to show how Dr. Goldenberg's proffered testimony would negate Thompson's specific intent to commit fraud.

Because the bulk of Dr. Goldenberg's opinion is irrelevant to the issue of Thompson's intent, the portions identified above should be excluded as irrelevant, prejudicial, misleading, confusing, and inflammatory under Fed. R. Evid. 401, 402, and 403. Additionally, many of his opinions and observations are not helpful to the jury and therefore do not meet the threshold for admissibility under Rule 702 and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

The government also notes that Dr. Goldenberg's opinion regarding Thompson's mental health is misleading because it is incomplete. The complete evidence regarding Thompson's mental health in this case has the potential to cut both ways. Dr.

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Goldenberg's opinion touches on aspects of Thompson's mental health that could be expected to garner sympathy, such as details about past trauma she has experienced. But Dr. Goldenberg's opinion ignores indications of Thompson's mental health that would not be expected to garner sympathy, such as her threats to hold people hostage and commit mass shootings, combined with pages of Google searches for firearms and firearm accessories.[5]

There is evidence that revenge was a motivating factor in Thompson's hacking scheme, and threats to harm other people are consistent with a revenge motive. For example, in its case-in-chief, the government intends to admit the following series of Twitter messages that Thompson wrote:

> And im gonna set a fucking example for the next mother fucker who wants to play lets see how much i can get away with a kid . . . . its gonna be ugly.
>
> Oh yeah and this duncan smith aka astrid piece of shit that he fucking turned against me too, add that mother fucker to the hit list.
>
> Yea this data that i stole straight outta s3 cos im just so incompetent, wouldnt a fuckin happened if this mother fucker, had just left me the fuck alone.
>
> Yeah im doing this its all archived, ready to upload to mega / Im gonna give it to darkness, that piece of shit I wouldnt be surprised if hes one of tp's fucking piece of shit kronies too.
>
> Im gonna give I to worse people too, im gonna give it to an avid scammer, a chinaman who will find a good perm home for it on the black market, sealed with the story behind it.

Despite the evidence that suggests Thompson's hacking scheme was motivated by revenge, the government does not intend to offer "other acts" evidence of Thompson's threats to physically harm others or her searches related to firearms in its case-in-chief. However, those threats properly will be a subject of cross-examination or rebuttal if the

[5] The omission of these details is not surprising; Dr. Goldenberg was retained to provide an opinion relevant to the question of how continued pretrial detention might impact Thompson's mental health and he did not opine on her "other acts" or what may have motivated her to commit the crimes with which she is charged.

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

defense opens the door to Thompson's mental health conditions and their manifestations in the defense case. It would be fundamentally unfair and misleading for the defense to raise aspects of Thompson's background that are likely to garner sympathy without allowing the government to raise aspects of Thompson's background that are consistent with an intent to harm others. Both categories of evidence contribute to a full picture of her mental health.

As a final point, providing an incomplete picture of Thompson's mental health and its effect on her criminal intent will only move the jury's focus from the issues in the case to collateral side issues. This will add significantly to the length of the trial while adding nothing to the jury's determination of guilt or innocence.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, STE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

I. CONCLUSION

For all the above-stated reasons, the Court should grant the government's motions *in limine* to exclude irrelevant and prejudicial evidence and argument.

May 27, 2022

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

s/ Andrew C. Friedman
s/ Jessica M. Manca
s/ Tania M. Culbertson
ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, WA 98101
Phone: (206) 553-7970
Fax: (206) 553-0882
Email: andrew.friedman@usdoj.gov
jessica.manca@usdoj.gov
tania.culbertson@usdoj.gov